UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,812	11/21/2003	Terrence A. Tomkow	RPOST-66232	3326

24201 7590 08/26/2008

FULWIDER PATTON LLP
HOWARD HUGHES CENTER
6060 CENTER DRIVE, TENTH FLOOR
LOS ANGELES, CA 90045

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/719,812	TOMKOW, TERRENCE A.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24,26-28,30-40 and 43-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24,26-28,30-40 and 43-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 7/1/2008.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/1/2008 has been entered.

Response to Arguments

Applicant's arguments filed 7/1/2008 have been fully considered but they are not persuasive.

Regarding the applicant's argument, with respect to claim 24, that Tomkow does not disclose the step of providing at the server a compressed encrypted version of the received message, the examiner does not find the argument persuasive. Tomkow disclosed on page 41 Lines 30-32 that the registered version of the message is presented to the system (server). Page 40 Lines 26-30 show that the registered version of the message includes "a digital signature or encrypted message digest", both of which read on a compressed encrypted version of the message. Further, the claim only requires that this be "providing at the server", and does not require that it had been previously stored, or subsequently generated by the server. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claim 24, that Tomkow did not disclose decompressing the message to obtain a first digital fingerprint and then decrypting the compressed encrypted version of the message provided at the server to provide a second digital fingerprint for comparison, the examiner does not find the argument persuasive. Note that the examiner has interpreted the hash of Tomkow to the digital signature of the claimed invention. Tomkow Page 41 Line 32 – Page 42 Line 5 clearly teaches generating a hash from the document (this reads on the decompressing the message to obtain a first digital fingerprint), and decrypting the digital signature, which was included with the registered version of the message, to obtain another hash (this reads on the decrypting the compressed encrypted version of the message…to obtain a second digital fingerprint). This passage further clearly teaches comparing the two hashes (digital fingerprints) for equality. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claim 1, that Meyer does not teach or suggest generating a digital signature of the message at the server, attaching the digital signature to an attachment that is not part of the message at the server, and then attaching the message to the recipient, the examiner does not find the argument persuasive. As discussed below, this newly claimed limitation is met by Tomkow. Furthermore, Meyer does teach attaching the meta-content of an email message to an HTML file and then attaching the HTML file to the message, as can be seen in paragraphs 0094-0095. Therefore the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claim 40, that neither Tomkow nor Meyer teach "digitally sealing" the encrypted hash of the hashed string "by attaching the

encrypted hash of the hashed string to an HTML file…", the examiner does not find the argument persuasive. While neither reference specifically teaches such, the ordinary person of skill in the art at the time of invention, who was also of ordinary creativity in the art, would have recognized that the encrypted digital signature of Tomkow (which reads on the encrypted hash of the hashed string) is meta-content (content about the content) of the message, and as Meyer teaches including the meta-content of email messages in an meta-content index attached to the email, it would have obvious to have done so. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claim 33, that Tomkow does not teach sending an attachment that is not part of the message, the examiner does not find the argument persuasive. Tomkow is not relied upon alone in meeting this limitation, but instead the combination of Tomkow and Meyer render this limitation obvious. See the rejection of claim 1. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claim 33, that Tomkow does not disclose providing at a server a compressed encrypted version of the combination of the message and the attachment…and then comparing the first and second digital fingerprints of the combination of the message and the attachment to determine the authenticity of the message and the attachments, the examiner does not find the argument persuasive. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Further, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references

individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Stark renders obvious the compressing and decompressing of the "encrypted version of the combination of the message and the attachment" (See Tomkow Encrypted Digital Signature). This forms a "first fingerprint", which is the encrypted digital signature. Tomkow teaches that the encrypted digital signature is then decrypted, which forms a "second fingerprint", as can be seen on Page 41 Lines 32-33. The second fingerprint is compared with a generated fingerprint in order to determine the authenticity of the message and the attachment, as can be seen on Page 41 Line 32 - Page 42 Line 5. This comparison of the second fingerprint is also a comparison of the first fingerprint, as the first fingerprint contains the same data as the second fingerprint, but in a different form. Further, the claim language does not require "comparing the first fingerprint to the second fingerprint for equality", but rather requires that the two fingerprints are compared to something. The examiner's interpretation of the claim language is also consistent with the teachings of the instant specification. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument, with respect to claims 38-39, that the combination of Tomkow and Kaufman did not teach "digitally sealing the encrypted hashed string by attaching the encrypted hashed string to an HTML file and attach the HTML file including the encrypted hashed string to the message", the examiner does not find the argument persuasive. First, the applicant has completely ignored the fact that Meyer was also relied upon in rejecting these claims. This is due to the fact that, as discussed above, Meyer renders obvious placing the encrypted digital signature in an HTML file attached to the email message. Furthermore, simply

because the references relied upon in rejecting the claim language do not specifically use the terms "digitally sealing", they render obvious " by attaching the encrypted hashed string to an HTML file and attach the HTML file including the encrypted hashed string to the message", and as such meet the limitations of the claim language. As such, the examiner does not find the argument persuasive.

Applicant's arguments with respect to the remaining claims have been considered but are moot in view of the new ground(s) of rejection.

Claims 1-24,26-28,30-40 and 43-46 have been examined.

Claim Objections

Claims 1-7, 10-13, 19-20, and 38-39 are objected to because of the following informalities:

Regarding claim 1 and its dependants, claim 1 recites the limitation "the attachment", however the claim language refers to two different attachments, and as such it is not clear which attachment is being referred to by the claim language. The examiner will assume for the purposes of searching prior art that either of the two attachments will meet the limitation of "the attachment".

Regarding claim 10 and its attachments, claim 10 recites "the steps at the server of: transmitting to the server from the recipient", which does not makes sense. This implies that the server transmits the message to itself from the recipient. The examiner has assumed, based upon the specification, for purposes of searching prior art, that this limitation was meant to read "the steps at the server of: receiving at the server from the recipient".

Regarding claims 38 and 39, claim 38 was labeled as "Currently Amended" but does not appear to have been amended.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 24 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow (WO 01/10090).

Regarding claim 24 , Tomkow disclosed in a method of transmitting a message from a sender to a recipient through a server displaced from the recipient (See Tomkow Abstract), the steps at the server of: receiving the message from the recipient at a web site providing at the server for an indication of the authenticity of the message (See Tomkow Page 41 Lines 28-32); providing at the server a compressed encrypted version of the message where the compression is a particular compression and the encryption is a particular encryption (See Tomkow Page 41 Lines 30-32); decompressing the message in accordance with the particular compression to provide a first digital fingerprint of the message (See Tomkow Page 42 Lines 1-2); decrypting the compressed encrypted version of the message in accordance with the particular encryption to provide a second digital fingerprint of the message (See Tomkow Page 41 Lines 30-32); and

comparing the first and second digital fingerprints of the message to determine the authenticity of the message (See Tomkow Page 42 Lines 2-15).

Regarding claims 26 Tomkow disclosed that the message is received at the server through the internet and wherein the message and the digital signature of the message are transmitted to the recipient through the internet, and that the state of authenticity of the message is transmitted through the internet to the recipient (See Tomkow Page 43 Lines 3-28).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-23, 27-28, 30-32, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow, and further in view of Meyer et al. (Patent Application Publication US 2002/0143871) hereinafter referred to as Meyer.

Regarding claims 1, 8, and 14, Tomkow disclosed a method of transmitting a message from a sender to a recipient through a server displaced from the recipient (See Tomkow Abstract), including the steps at the server of: receiving the message at the server from the sender (See Tomkow Page 29 Lines 16-18), generating at the server a digital signature of the message (See Tomkow Page 29 Lines 28-29), attaching the digital signature of the message to the

message, the attachment including the identity of the sender in plain text (See Tomkow Page 40 Lines 19-31), transmitting from the server to the recipient the message and the attachment (See Tomkow Page 40 Lines 30-31), receiving the message and the attachment at the server from the recipient (See Tomkow Page 41 Lines 29-32), providing digital signatures of the message and the attachment at the server (See Tomkow Page 41 Line 32 – Page 42 Line 2), and authenticating to the recipient the message and the attachment at the server on the basis of the information received by the recipient from the server and on the basis of the digital signatures provided by the server (See Tomkow Page 41 Line 28 – Page 42 Line 15), but Tomkow failed to specifically disclose that the attachment was an HTML file, or generating the HTML file at the server.

Meyer teaches that in an email server, meta-content can be added in the form of an html attachment to a email by (1) separating the email body from the header, (2) extracting the email send date, (3) extracting various named entities, (4) executing a summarization process to produce a document summary, (5) normalization of dates and currency, (6) color-encoding dates, (7) sorting and displaying dates, (8) annotation by color-coding, (9) creating hyperlinks to external HTML documents, and (10) converting special characters to HTML ampersand characters (See Meyer Fig. 1 and Fig. 7a and Paragraph 0091-0095).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Meyer in the E-mail system of Tomkow, by attaching an HTML index attachment to each email at the RPost Server, the HTML index attachment containing the meta-content from the email message. This would have been obvious because the ordinary person skilled in the art would have been motivated to simplify the use and management of the e-mails for recipients. It further would have been obvious to the ordinary

person skilled in the art to have included the digital signatures/message digests in the HTML index attachment. This would have been obvious because the ordinary person skilled in the art would have recognized the digital signatures/message digests as meta-content, and would have been motivated to include the meta-content in the HTML index attachment. Further still, it would have been obvious in this combination that the meta-content index would have been digitally signed and verified by the system, because Tomkow disclosed that the message and all attachments would be signed and verified (See Tomkow Page 40 Lines 19-31).

Regarding claim 27, Tomkow disclosed in a method of transmitting a message from a sender to a recipient through a server displaced from the recipient (See Tomkow Abstract), the steps at the server of: receiving the message from the recipient at a web site providing at the server for an indication of the authenticity of the message (See Tomkow Page 41 Lines 28-32); providing a compressed encrypted version of the message where the compression is a particular compression and the encryption is a particular encryption (See Tomkow Page 41 Lines 30-32); receiving an attachment from the recipient at the website where the reception of the attachment is at the same time as the reception of the message and the attachment contains information about delivery of the message to the recipient (See Tomkow Page 41 Line 28 – Page 42 Line 15) decompressing the message in accordance with the particular compression to provide a first digital fingerprint of the message (See Tomkow Page 42 Lines 1-2); decrypting the compressed encrypted version of the message in accordance with the particular encryption to provide a second digital fingerprint of the message (See Tomkow Page 41 Lines 30-32); and comparing the first and second digital fingerprints of the message to determine the authenticity of the message (See Tomkow Page 42 Lines 2-15), Tomkow failed to disclose that the attachment was separate

from the message, that the attachment was in the form of an HTML file, or that the HTML file included a digital signature of the message. But Tomkow did disclose that the registered message included an attached digital signature of the message (See Tomkow Page 40 Lines 19-31).

Meyer teaches that in an email server, meta-content can be added in the form of an html attachment to a email by (1) separating the email body from the header, (2) extracting the email send date, (3) extracting various named entities, (4) executing a summarization process to produce a document summary, (5) normalization of dates and currency, (6) color-encoding dates, (7) sorting and displaying dates, (8) annotation by color-coding, (9) creating hyperlinks to external HTML documents, and (10) converting special characters to HTML ampersand characters (See Meyer Fig. 1 and Fig. 7a and Paragraph 0091-0095).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Meyer in the E-mail system of Tomkow, by attaching an HTML index attachment to each email at the RPost Server, the HTML index attachment containing the meta-content from the email message. This would have been obvious because the ordinary person skilled in the art would have been motivated to simplify the use and management of the e-mails for recipients. It further would have been obvious to the ordinary person skilled in the art to have included the digital signatures/message digests in the HTML index attachment. This would have been obvious because the ordinary person skilled in the art would have recognized the digital signatures/message digests as meta-content, and would have been motivated to include the meta-content in the HTML index attachment. Further still, it would have been obvious in this combination that the meta-content index would have been

digitally signed and verified by the system, because Tomkow disclosed that the message and all attachments would be signed and verified (See Tomkow Page 40 Lines 19-31).

Regarding claim 40, Tomkow disclosed in a method of transmitting a message and an attachment from a sender through a server displaced from the recipient, the steps at the server of: identifying the sender (See Tomkow Page 16 Line 10 – Page 17 Line 5), providing the attachment and the message stripped of the attachment (See Tomkow Page 29 Lines 21-31), providing a string formed from the identification of the sender, the attachment and the message stripped of the attachment (See Tomkow Page 40 Lines 19-31), and hashing the string (See Tomkow Page 40 Lines 19-31), encrypting the hash of the hashed string (Tomkow Page 40 Lines 19-31); digitally sealing the encrypted hash of the hashed string by attaching the encrypted hash of the hashed string to [the email] (See Tomkow Page 40 Lines 19-31); and sending to the recipient the message and the encrypted hash of the hash string (Tomkow Page 40 Lines 19-31), but Tomkow failed to disclose attaching the hash to an HTML file or sending the HTML file including the hash.

Meyer teaches that in an email server, meta-content can be added in the form of an html attachment to a email by (1) separating the email body from the header, (2) extracting the email send date, (3) extracting various named entities, (4) executing a summarization process to produce a document summary, (5) normalization of dates and currency, (6) color-encoding dates, (7) sorting and displaying dates, (8) annotation by color-coding, (9) creating hyperlinks to external HTML documents, and (10) converting special characters to HTML ampersand characters (See Meyer Fig. 1 and Fig. 7a and Paragraph 0091-0095).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Meyer in the E-mail system of Tomkow, by attaching an HTML index attachment to each email at the RPost Server, the HTML index attachment containing the meta-content from the email message. This would have been obvious because the ordinary person skilled in the art would have been motivated to simplify the use and management of the e-mails for recipients. It further would have been obvious to the ordinary person skilled in the art to have included the digital signatures/message digests in the HTML index attachment. This would have been obvious because the ordinary person skilled in the art would have recognized the digital signatures/message digests as meta-content, and would have been motivated to include the meta-content in the HTML index attachment. Further still, it would have been obvious in this combination that the meta-content index would have been digitally signed and verified by the system, because Tomkow disclosed that the message and all attachments would be signed and verified (See Tomkow Page 40 Lines 19-31).

Regarding claim 2, Tomkow and Meyer disclosed that the server creates digital fingerprints from the digital signatures and from the message and the attachment to authenticate the message and the attachment on the basis of the digital fingerprints (See Tomkow Page 12 Lines 1-6 and Page 29 Lines 21-26 and Page 40 Lines 19-31, and Page 41 Line 32 – Page 42 Line 15).

Regarding claim 3, Tomkow and Meyer disclosed that the attachment includes interim stations between the recipient and the server (See Tomkow Page 2 Lines 1-3) and wherein the message and the attachment, and the digital signatures of the message and the attachment, are transmitted from the server to the sender to provide for a determination at the server for the

sender of the authenticity of the message and the attachment (See Tomkow Page 22 Line 14 – Page 23 Line 30).

Regarding claim 4, Tomkow and Meyer disclosed that the message and the attachment and the digital signatures of the message and the attachment are not retained at the sender when the message and the attachment and the digital signatures are transmitted from the server to the sender (See Tomkow Page 25 Lines 15-21).

Regarding claim 5, Tomkow and Meyer disclosed that the message and the attachment and the digital signatures of the message and the attachment are transmitted from the server to the sender (See Tomkow Page 22 Line 15 – Page 23 Line 30).

Regarding claim 6, Tomkow and Meyer disclosed that the sender transmits to the server, to authenticate the message, the information supplied by the server to the sender and wherein the server operates upon the information from the sender to authenticate the message (See Tomkow Page 26 Line 1 – Page 28 Line 4).

Regarding claim 7, Tomkow and Meyer disclosed that the message and the digital signature of the message are discarded after the message and the digital signature are transmitted by the server to the sender (See Tomkow Page 25 Lines 4-16).

Regarding claim 9, Tomkow and Meyer disclosed transmitting to the recipient the state of authenticity of the message on the basis of the results of the comparison of the digital fingerprints (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claim 10, Tomkow and Meyer disclosed transmitting to the server from the recipient the message and the attachment (See Tomkow Page 41 Lines 28-32), and receiving from the sender the message and the attachment and the digital signatures of the message and the

attachment, producing digital fingerprints of the message, the attachment and the digital signatures, and comparing the digital fingerprints relating to the message, and the digital fingerprints relating to the attachment, to determine the authenticity of the message and the attachment (See Tomkow Page 26 Line 1 – Page 28 Line 4).

Regarding claim 11, Tomkow and Meyer disclosed disposing of the message and the attachment and the digital signatures of the message and the attachment after transmitting this information to the sender (See Tomkow Page 25 Lines 4-16).

Regarding claim 12, Tomkow and Meyer disclosed at the server: providing at the server, at the same time as the reception of the message, an attachment including the identity of the sender and the identity and address of the server and the identity and address of the recipient and the time of transmission of the message from the server to the recipient (See Tomkow Page 30 Line 14 – Page 31 Line 26), transmitting from the server to the recipient the attachment at the same time as the transmission of the message (See Tomkow Page 30 Line 14 – Page 31 Line 26), and receiving from the recipient at the server the message and the attachment (See Tomkow Page 30 Line 14 – Page 31 Line 26), providing digital fingerprints of the message, the attachment and the digital signatures of the message and the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15), providing an indication of the authentication of the attachment on the basis of a comparison at the server of the digital fingerprints relating to the message and the digital fingerprints relating to the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claim 13, Tomkow and Meyer disclosed transmitting from the server to the recipient an indication of the authenticity of the message on the basis of the comparison of the

digital fingerprints relating to the message and the digital fingerprints relating to the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claim 15, Tomkow and Meyer disclosed that digital fingerprints are provided at the server of the message and the attachment and digital fingerprints are provided at the server of the digital signatures of the message and the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15) and wherein a comparison is provided at the server of the digital fingerprints of the message and the digital signature of the message, and the attachment and the digital signature of the attachment, to determine the authenticity of the message and the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claim 16, Tomkow and Meyer disclosed that the indications of the state of authenticity of the message and the attachment are transmitted from the server to the recipient (See Tomkow Page 41 Line 28 – Page 42 Line 15) and wherein the message and the attachment and the digital signatures of the message and the attachment are discarded at the server when the indications of the authenticity of the message and the attachment are transmitted from the server to the recipient (See Tomkow Page 35 Lines 11-13).

Regarding claim 17, Tomkow and Meyer disclosed that the message and the attachment and the digital signatures of the message and the attachment are transmitted from the server to the sender and wherein the server produces digital fingerprints of the message and the attachment and digital fingerprints of the digital signature of the message and the attachment and wherein the server compares the digital fingerprints relating to the message, and the digital fingerprints relating to the attachment, to determine the authenticity of the message and the attachment (See Tomkow Page 22 Line 14 – Page 23 Line 30 and Page 26 Line 1 – Page 28 Line 4).

Regarding claim 18, Tomkow and Meyer disclosed that the server transmits to the recipient the results of the comparison and wherein the server discards the message and the attachment and the digital signatures of the message and the attachment when the server transmits the message and the attachment and the digital signature of the message and the attachment to the recipient (See Tomkow Page 25 Line 3 – Page 28 Line 4).

Regarding claim 28, Tomkow and Meyer disclosed transmitting to the recipient the results of the comparison of the first and second digital fingerprints of the message and the first and second digital fingerprints of the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claims 19-23, 30, 31 Tomkow and Meyer disclosed that the message is received at the server through an internet and wherein the message and the digital signature of the message are transmitted to the recipient through the internet, and that the state of authenticity of the message is transmitted through the internet to the recipient (See Tomkow Page 43 Lines 3-28).

Regarding claim 32, Tomkow and Meyer disclosed the attachment includes the identity of the sender and the identity and the address of the server and the identity and address of the recipient and the time of transmission of the message from the server to the recipient (See Tomkow Page 30 Line 14 – Page 31 Line 26).

Claim 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and further in view of Menezes et al. (Handbook of Applied Cryptography), hereinafter referred to as Menezes.

Regarding claim 46, Tomkow disclosed in a method of authenticating at a recipient a message and an attachment transmitted from a sender to the recipient, providing an attachment (See Tomkow Page 41 Lines 19-32), providing at the recipient an encryptment of a string including information relating to the identification of the sender, the attachment and the message stripped of the attachment (See Tomkow Page 41 Lines 19-32), decrypting the encrypted hash of the hashed string (See Tomkow Page 41 Lines 32-33), separating the hash from the string (See Tomkow Page 42 Line 1), forming a hash from the information relating to the identification of the sender, the attachment and the message stripped of the attachment (See Tomkow Page 42 Lines 1-2), comparing the hash separated from the string and the hash formed from the information in the string (See Tomkow Page 42 Lines 2-15), and using the results of the comparison to indicate to the recipient the authenticity of the message and the attachment (See Tomkow Page 42 Lines 2-15), but Tomkow failed to disclose that the encrypted string was compressed, or decompressing the encrypted string.

Menezes teaches encryption provides confidentiality (See Menezes Section 1.2 "Cryptographic Goals".

It would have been obvious to the ordinary person skilled in the art at the time of invention to have encrypted the registered message prior to transmitting it to the recipient, and for the recipient to have decrypted the registered message. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure the confidentiality of the registered message.

Claims 43-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and Menezes, and further in view of Stark et al (Patent Application Publication 2002/0131566) hereinafter referred to as Stark.

Regarding claim 43, Tomkow and Menezes disclosed in a method of authenticating at a recipient a message and an attachment transmitted from a sender to the recipient through a server displaced from the recipient, the steps of: providing at the recipient an encrypted string including an identification of the sender, the message, a hash of the attachment, and an embedded hash of the string (See Tomkow Page 40 Lines 19-32 and the rejection of claim 46 above), decrypting the string (See the rejection of claim 46 above), hashing the string less the embedded hash of the string (See Tomkow Page 42 Line 1), comparing the hash of the string less the hash of the string and the embedded hash (See Tomkow Page 42 Lines 1-2), and using the results of the comparison to indicate to the recipient the authenticity of the message and the attachment (See Tomkow Page 42 Lines 2-15), but Tomkow failed to disclose that the string was compressed and encrypted, or decompressing and decrypting the compressed and encrypted string.

Stark teaches that in order to make email data smaller, the data should be compressed to make it smaller prior to transmission, and should be decompressed upon reception (See Stark Abstract).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Stark in the email system of Tomkow and Menezes by compressing the encrypted string, and later decompressing the encrypted string in order to allow for comparison. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to provide a smaller message for transmission.

Regarding claim 44, Tomkow, Menezes, and Stark disclosed separating the attachment from the message, hashing the separated attachment, comparing the hashed separated attachment and the hashed attachment in the string, and using the results of the comparison provided in the previous step to indicate the authenticity of the message and the attachment (See Tomkow Page 41 Line 19 – Page 42 Line 15).

Regarding claim 45, Tomkow, Menezes and Stark disclosed recovering the message and the attachment and transmitting the recovered message and attachment to the recipient with the indication of their authenticity (See Tomkow Page 41 Lines 19-25).

Claims 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and Meyer, and further in view of Stark et al (Patent Application Publication 2002/0131566) hereinafter referred to as Stark.

Regarding claim 33, Tomkow and Meyer disclosed an a method of transmitting a message from a sender through a server displaced from the recipient, the steps at the server of: receiving the message and an attachment in the form of an HTML file that is not part of the message from the recipient at a website providing at the server for an indication of the authenticity of the message, the attachment including a digital signature of the message (See Tomkow Page 41 Lines 28-32 and the rejection of claim 1 above), providing at the server for an encrypted version of the combination of the message and the attachment (See Tomkow Page 41 Lines 19-32), decrypting the encrypted version of the combination of the message and the attachment in accordance with the particular encryption to provide a digital fingerprint of the combination of the message and the attachment (See Tomkow Page 41 Lines 32-33), and

comparing second digital fingerprint to determine the authenticity of the message and the attachment (See Tomkow Page 42 Lines 1-5), but Tomkow and Meyer failed to disclose that the encrypted version was also compressed, decompressing the compressed encrypted version of the combination of the message and the attachment in accordance with the particular compression to provide a first digital fingerprint of the combination of the message and the attachment for comparison.

Stark teaches that in order to make email data smaller, the data should be compressed to make it smaller prior to transmission, and should be decompressed upon reception (See Stark Abstract).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Stark in the email system of Tomkow by compressing the modified message, and later decompressing the modified message in order to allow for comparison. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to provide a smaller message for transmission.

Regarding claim 34, the combination of Tomkow and Meyer and Stark disclosed transmitting to the recipient the results of the comparison of the first and second digital fingerprints (See Tomkow Page 41 Line 28 – Page 42 Line 15).

Regarding claim 35, see the rejection of claim 19 above.

Regarding claims 36 and 37, see the rejection of claim 29 above.

Claims 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow and Meyer, and further in view of Kaufman et al. (US Patent Number 5,764,772) hereinafter referred to as Kaufman.

Regarding claim 38, Tomkow and Meyer disclosed in a method of transmitting a message and an attachment from a sender to a recipient through a server displaced from the recipient, including the steps at the server of identifying the sender (See Tomkow Page 40 Lines 19-24), hashing the attachments (See Tomkow Page 40 Lines 21-25), stripping the message of the attachments, hashing the identification of the sender, the hashed attachments and the message to form a hashed string (See Tomkow Page 40 Lines 22-26), encrypting the hashed string (See Tomkow Page 40 Lines 26-28), and digitally sealing the encrypted hashed string by attaching the encrypted hashed string to an HTML file and attaching the HTML file including the encrypted hashed string to the message (See Tomkow Page 40 Lines 26-30 and the rejection of claim 1 above), but Tomkow and Meyer failed to disclose hashing the hashed string and encrypting the result if the hashing of the hashed string.

Kaufman teaches that in order to protect against the use of a lookup table to compute hashes, the hash should be performed multiple times (See Kaufman Col. 10 Line 64-Col. 11 Line 6).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaufman by hashing the hashes of Tomkow. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent the generation of a hash table corresponding to the hashing system.

Regarding claim 39, Tomkow, Meyer, and Kaufman disclosed adding the message to the encrypted hash of the hashed string, and transmitting the message and the encrypted hash of the hashed string to the recipient (See Tomkow Page 40 Lines 26-31).

Conclusion

Claims 1-24,26-28,30-40 and 43-46 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/

Primary Examiner, Art Unit 2131